Exercice d'arithmétique

~ Infophile ~

★★★

Énoncé :

Existe-t-il des entiers m et p tels que :

$$m^2 + (m+1)^2 = p^3$$

Autrement dit est-il possible que la somme de deux carrés d'entiers consécutifs soit un cube ?

Calculs Préliminaires

On transforme l'expression :

$$m^2 + (m+1)^2 = p^3 \iff 2m^2 + 2m + 1 = p^3 \iff (2m+1)^2 + 1 = 2p^3$$

Posons $n = 2m+1$ on cherche donc n tel que :

$$n^2 + 1 = 2p^3$$

On se place alors dans l'**anneau de Gauss** $\mathbb{Z}[i]$ et on se ramène à :

$$(n+i)(n-i) = (1+i)(1-i)p^3 \quad (*)$$

Lemme 1 :

Soit q un diviseur de p vérifiant $(*)$, irréductible dans $\mathbb{Z}$, alors q n'est pas irréductible dans $\mathbb{Z}[i]$.

Démonstration :

Raisonnons par l'absurde et supposons q est irréductible dans $\mathbb{Z}[i]$.

D'après Gauss $q|n+i$ ou $q|n-i$ donc $q|\overline{n+i}$ ou $q|\overline{n-i}$.

Ainsi $q|n+i$ **et** $q|n-i$ soit :

$$\exists \alpha \in \mathbb{Z}[i],\ q = \alpha(n+i)(n-i)$$

Par hypothèse :

$$q|p \iff \exists\beta \in \mathbb{Z}[i],\ p = \beta q$$

On reporte dans $(*)$:

$$(n+i)(n-i) = (1+i)(1-i)\beta^3 q^2 \times \alpha(n+i)(n-i)$$

Par intégrité on peut simplifier par $(n+i)(n-i)$:

$$1 = (1+i)(1-i)\beta^3\alpha q^2 \implies q|1$$

Or q est irréductible dans $\mathbb{Z}$, d'où la **contradiction**.

$\square$

Lemme 2 :

Soit q un diviseur de p vérifiant $(*)$, irréductible dans $\mathbb{Z}$, alors q est somme de deux carrés.

Démonstration :

La *norme* dans cette anneau est définie par :

$$\forall(a,b) \in \mathbb{Z}^2,\ N(a+ib) = a^2 + b^2$$

On montre qu'elle est multiplicative, c'est-à-dire que :

$$\forall(x,y) \in \mathbb{C}^2,\ N(x.y) = N(x).N(y)$$

D'après le lemme 1. q n'est pas irréductible dans $\mathbb{Z}[i]$ donc :

$$\exists(a,b) \in \mathbb{Z}[i]^2,\ q = ab$$

On passe à la norme :

$$N(q) = N(ab) = N(a)N(b)$$

Et puisque $q \in \mathbb{Z}$ on a $N(q) = q^2$ d'où :

$$N(a)N(b) = q^2$$

Or q irréductible dans $\mathbb{Z}$ donc $N(a) = N(b) = q$ et par conséquent :

$$\boxed{q = \Re(a)^2 + \Im(a)^2}$$

$\square$

Fin de la démonstration

En conséquence on a p de la forme :

$$p = \prod(a_k^2 + b_k^2) = \prod(a_k + ib_k)(a_k - ib_k)$$

On réécrit alors $(*)$:

$$(n+i)(n-i) = (1+i)(1-i)\prod(a_k + ib_k)^3(a_k - ib_k)^3 \quad (\circledast)$$

Considérons deux éléments conjugués du produit mettons $a_1 + ib_1$ et $a_1 - ib_1$.

$$\Rrightarrow a_1 + ib_1 \text{ (resp. } a_1 - ib_1) \text{ divise } n+i \text{ ou } n-i$$

$$\Rrightarrow n+i \text{ est divisible par } \prod(a_k \pm ib_k)$$

On a alors :

$$\begin{cases} n+i = \lambda\prod(a_k \pm ib_k)^3 \\ n-i = \overline{\lambda}\prod(a_k \mp ib_k)^3 \end{cases}$$

On reporte dans $(\circledast)$ et on simplifie :

$$\lambda\overline{\lambda} = (1+i)(1-i)$$

Puisque l'anneau est factoriel et que $(1+i)$ et $(1-i)$ sont irréductibles on a :

$$\begin{cases} \lambda = 1+i \\ \overline{\lambda} = 1-i \end{cases} \quad \text{ou} \quad \begin{cases} \lambda = 1-i \\ \overline{\lambda} = 1+i \end{cases}$$

On pose $\prod(a_k + ib_k) = (a+ib)$ et donc :

$$n+i = (1+i)(a+ib)^3 \quad \text{ou} \quad n+i(1-i)(a+ib)^3$$

Traitons le premier cas, le second se traitant de la même manière.

Les parties imaginaires donnent :

$$1 = a^3 - 3ab^2 + 3a^2b - b^3 = (a-b)((a-b)^2 + 6ab)$$

D'où deux cas :

$$\begin{cases} a-b = 1 \\ (a-b)^2 + 6ab = 1 \end{cases} \quad \text{ou} \quad \begin{cases} a-b = -1 \\ (a-b)^2 + 6ab = -1 \end{cases}$$

Le deuxième système n'a pas de solutions, et le premier donne :

$$\begin{cases} a = 1 \\ b = 0 \end{cases} \quad \text{ou} \quad \begin{cases} a = 0 \\ b = -1 \end{cases}$$

On obtient (en tenant compte de l'étude du second cas) $n = 1$ ou $n = -1$.

On en conclut que les seuls couples d'entiers vérifiant la relation sont :

$$\boxed{(m,p) = (0,1) \quad \text{ou} \quad (m,p) = (-1,1)}$$

■